

3. European Patent application 99 114 740.6, published as EP1073257A1, Method for generating a security document, inventors R.D.Hersch, N. Rudaz, filed July 28, 1999.

Orell Füssli Security Printing Ltd.

Zürich

**Method for generating a security document**

## Method for generating a security document

The present invention relates to a method for generating a security document and to a security document  
5 obtained by this method according to the preamble of the independent claims. In particular, it relates to the field of security printing, and more particularly it relates to anti-counterfeiting measures for identity documents showing a photograph of their holder.

10 Many identity documents bear a photograph of the document holder, because this photograph offers a convenient way of relating the document to its owner. The development of plastic card printers and the advances in digital imagery have lead to the widespread use of identity documents printed on plastic cards, such as ID  
15 cards, driving licenses and access key cards.

With the advance of color printers and copiers, it has become easy to forge such documents unless they are provided with security features, such as digital  
20 watermarks, microscopic text, etc. Such security features are, however, difficult to apply or to verify and they often impair the overall appearance of the document.

The problem to be solved by the present application lies therefore in avoiding at least part of  
25 these advantages. This problem is solved by the independent claims.

Hence, at least some of the points of the original image are modified by changing their color. The change of color is a function of the original color  $C_{ij}$ ,  
30 of the value  $p_{ij}$  of a security pattern as well as of a local average  $\alpha_k$  of the pattern. By using a function that depends on a local average of the pattern, it becomes possible to generate very flexible security markings that take the pattern's features into account. The protected  
35 image is difficult to imitate by using commercial image-processing packages because the changes in the protected image do not occur along a fixed direction of the color

space, but vary according to the color of the original image pixels and the averages of the security pattern.

The embedded pattern can e.g. be textual information already present elsewhere on the document, or  
5 it can be a code derived from data specific to the document holder. The protection can be made fully apparent, partly apparent, or completely invisible under normal viewing conditions.

In a preferred aspect of the invention, a  
10 chromatic shift is given for any color of the original image. This shift is defined by the two colors that are used when the pattern value takes its minimum and maximum values. In this case, the function  $f$  can e.g. consist of a linear interpolation between the two colors of the  
15 chromatic shift.

The chromatic shift can be derived from a reference shift at one specific color  $K$ . Preferably, a correcting offset is applied to this reference shift for balancing it according to the local average  $\alpha_K$  of the  
20 pattern. The chromatic shift can be calculated by correcting the luminance, hue and saturation of the reference shift (or the corrected reference shift). A further possible correction adjusts the values of the chromatic shift to make its CIE-Lab luminance difference equal to  
25 the one of the reference shift, which results in a uniformly bright pattern for any original color value.

The protected image is difficult to reproduce through photo-mechanic means such as a photocopying device, because the chromatic shifts it contains can be  
30 specified as quasi-metameric pairs of colors. Either the pairs of colors are perceived as identical by the device and the embedded information is completely lost, or the pairs of colors are perceived as being more different than they really are and the embedded information becomes  
35 much more visible under normal light than it is in the protected image.

Identity documents containing images with embedded text are even more difficult to forge, because the embedded text can contain an encrypted version of the personal information present elsewhere on the document.

5 Without knowledge of the process used for encrypting the text, it is impossible to adapt an existing document to a fake identity by replacing the photograph and the personal information.

10 The invention is especially suited for marking identity documents, such as driver's licenses.

Further preferred features and embodiments are described in the dependent claims as well as in the description, which makes reference to the figures. These show:

15 Fig. 1 a single character and its corresponding gray level (top row) as well as the equality of two areas having the same local average,

Fig. 2 the LEF color space,

Fig. 3 a bitmap pattern for a given string,

20 Fig. 4 the calculation of the average value for a letter bitmap,

Fig. 5 the balancing of the reference shift,

Fig. 6 the assembly of a text into its pattern,

25 Fig. 7 the repetitive arrangement of the pattern of Fig. 6,

Fig. 8 the repetitive arrangement of the pattern of Fig. 7,

30 Fig. 9 the staggering of the pattern on Fig. 8,

Fig. 10 the individual balanced reference shifts of differing letters,

Fig. 11 the horizontal interpolation of the reference shifts,

35 Fig. 12 the vertical interpolation of the reference shifts,

Fig. 13 the luminance correction,

Fig. 14 the hue correction,  
 Fig. 15 the saturation correction, and  
 Fig. 16 the overflow correction.

A preferred embodiment of a method that protects identity documents by embedding text into photographs is described hereafter. The method consists of the following basic steps: A reference chromatic shift (the "reference shift") is specified in a linear color space. Each character of the text to embed is rasterized into a  
 10 bitmap. The reference shift is corrected for obtaining a coverage-balanced chromatic shift ("corrected chromatic shift") derived for each rasterized character according to the ratio between the surface occupied by black pixels (foreground) and the surface occupied by white pixels  
 15 (background), i.e. according to a local average of the security pattern. The rasterized character string is repeated horizontally and vertically to form a security pattern. A pattern-relative chromatic shift is interpolated between the coverage-balanced chromatic shifts of  
 20 the neighboring bitmap characters for each pixel in the security pattern. A chromatically shifted color is extrapolated from the pattern-relative chromatic shifts for each pixel of the original image. The protected image is generated and output on a continuous-tone printer. De-  
 25 pending on the size and orientation of the reference chromatic shift, the embedded text in the protected image can be visible or invisible under normal viewing conditions.

30 Chromatic shifts:

A "chromatic shift" is defined as a set of three colors  $C$ ,  $C_b$  and  $C_f$  such that a surface of unitary area colored with  $C$  is visually equivalent to the same surface split in two foreground and background parts of  
 35 area  $\alpha$ , resp.  $1 - \alpha$ , with the foreground having color  $C_f$  and the background having color  $C_b$  (Fig. 1). Mathematically, the colors of a chromatic shift must verify the

relation  $C = \alpha C_f + (1 - \alpha) C_b$ ,  $C$  represents the reference color,  $C_b$  represents the reference background color, and  $C_f$  represents the reference foreground color.

5 An additive color space is used for specifying the colors of a chromatic shift. Preferably, this color space is obtained by a linear transformation of the cube formed by the RGB space. The transformation and its inverse are defined by the following equations:

$$10 \quad \begin{bmatrix} L \\ E \\ F \end{bmatrix} = \begin{bmatrix} \frac{2}{3} & \frac{2}{3} & \frac{2}{3} \\ 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{3}{2} & 0 \\ \frac{1}{2} & -\frac{1}{3} & \frac{1}{\sqrt{3}} \\ \frac{1}{2} & -\frac{1}{3} & -\frac{1}{\sqrt{3}} \end{bmatrix} \cdot \begin{bmatrix} L \\ E \\ F \end{bmatrix} \quad (1)$$

After transformation, the RGB cube stands on its black corner (Fig. 2). Its black-white axis is vertical and becomes the L-axis in the newly defined LEF color coordinate space. The two other E and F orthogonal axes are lying in the plane perpendicular to the L-axis through point  $L = 0$  (the EF-plane). The E-axis goes through the projection of vertex R of the RGB cube on plane EF. The vertical L component can be assimilated to the achromatic value of a given color, i.e. its luminance level. The E and F components convey the chromatic information pertaining to that color.

Choosing the reference shift:

25 The reference shift  $\{K, K_b, K_f\}$  for an arbitrary color  $K$  is specified by an interactive color picking application according to N. Rudaz, R. D. Hersch, V. Ostromoukhov, Specifying color differences in a linear color space (LEF), Proceedings of the IS&T/SID 97, 30 Scottsdale, 1997, pp. 197-202.

Creating a partial security pattern:

The string of characters forming the text to embed into the image is converted into a bitmap image through the use of a font rendering software component such as the FreeType engine described at the URL <http://www.freetype.org/intro.htm>.

The font rasterizer creates a rectangular bitmap for each character in the string of text (Fig. 3), which will form part of the security pattern.

Local averaging:

In the case of a binary bitmap, local averages  $\alpha_k$ , defined as the black coverage percentage, are calculated for each character bitmap.  $\alpha_k$  lies between 0 and 1; it is defined as the ratio between the number  $P_k$  of foreground pixels and total number  $P_k$  of pixels or, in other words, if a pattern value  $p_{ij}$  of 1 is assigned to the foreground pixels and a pattern value  $p_{ij}$  of 0 to the background pixels,  $\alpha_k$  corresponds to the average of the pattern values (Fig. 4).

Correcting the reference shift:

A coverage-balanced chromatic shift  $\{K, K_b', K_f'\}$  is derived from the reference shift  $\{K, K_b, K_f\}$  for each character bitmap. The chromatic distance  $D = K_b - K_f$  is computed. An offset  $d$  is derived from  $D$  using the relation

$$d = D \cdot (\alpha_k - (p_{\max} - p_{\min})/2) / (p_{\max} - p_{\min}).$$
 wherein  $p_{\min}$  and  $p_{\max}$  are the largest and smallest possible pattern values (for binary patterns we usually have  $p_{\max} = 1$  and  $p_{\min} = 0$ ).

This offset  $d$  is added to  $K_b$  and to  $K_f$  in order to obtain  $K_b'$  and  $K_f'$  (Fig. 5):

$$K_b' = K_b + d, \quad (2)$$

$$K_f' = K_f + d$$

The resulting coverage-balanced chromatic shift  $\{K, K_b', K_f'\}$  exhibits the property that, if the

white pixels of the associated character bitmap are colored with  $K_b'$  and the black pixels with  $K_f'$ , then the average color of the character bitmap is equal to  $K$ .

5                   Generating the security pattern:

                  The rasterized characters are horizontally juxtaposed into a rectangular tile (Fig. 6). This tile is horizontally repeated side by side as many times as necessary in order to produce a second bitmap with the same width as the original image (Fig. 7). The second bitmap is vertically replicated side by side as many times as necessary in order to produce a third bitmap image with the same height as the original image (Fig. 8). At each vertical repetition, the second bitmap is shifted horizontally in order to avoid disturbing optical artifacts that appear when characters are vertically aligned in a text. After the horizontal shift, the portion of the second bitmap that goes beyond the horizontal boundaries of the original image is wrapped around (Fig. 9). This third bitmap is referred to as the security pattern and constitutes an image of the text that will be embedded into the original image.

Calculating the pattern-relative chromatic shifts:

25                   A pattern-relative chromatic shift is computed for every pixel of the security pattern, based on the coverage-balanced chromatic shifts associated with the character bitmaps.

                  In a first step, every pixel of the security pattern that is located at the center of a character bitmap is associated with that bitmap's coverage-balanced chromatic shift (Fig. 10).

                  In a second step, every pixel of the security pattern that is located on a horizontal line segment joining two centers of the character bitmaps is associated with a pattern-relative chromatic shift that is obtained by linear interpolation between the coverage-



balanced chromatic shifts associated with these two centers (Fig. 11).

In a third step, every pixel of the security pattern that is located on a vertical line segment joining two pixels processed during the second step is associated with a pattern-relative chromatic shift that is linearly interpolated between the pattern-relative chromatic shifts of these two pixels (Fig. 12).

In a fourth step, every pixel of the security pattern that has not been processed during the previous steps is associated with the pattern-relative chromatic shift of its nearest neighbor.

#### Calculating the chromatic shift:

Each pixel in the security pattern is associated with a pixel having the same coordinates in the original image. The pattern-relative chromatic shift undergoes a geometrical transformation in the LEF color space, with the purpose of adapting its background and foreground colors ( $K_b'$  and  $K_f'$ ), so that the color resulting from the average  $\alpha_k$  of the adapted background and foreground colors is equal to the color  $C_{ij} = (L_C, E_C, F_C)$  of the associated original pixel.

In a first step, the luminance of the chromatic shift is corrected according to the luminance difference between the reference color  $K$  and the color  $C_{ij}$ . For this purpose, the luminance difference  $\Delta L_{CK}$  between  $C_{ij}$  and  $K = (L_K, E_K, F_K)$  is computed using the relation

$$\Delta L_{CK} = L_C - L_K, \quad (3)$$

and this luminance difference is added to  $K'$ ,  $K_b'$  and  $K_f'$  in order to obtain the colors  $K''$ ,  $K_b''$  and  $K_f''$  (Fig. 13).

In a second step, the hue of the chromatic shift is corrected according to the hue difference between the reference color  $K$  and the color  $C_{ij}$ . For this purpose, the angular hue difference ( $\Delta H_{CK}$ ) between  $C$  and  $K''$  is computed using the relation

$\Delta H_{CK} = \text{Tan}(\text{Arctan}(F_C/E_C) - \text{Arctan}(F_{K''}/E_{K''})), \quad (4)$   
 and this angular hue difference is added to  $K''$ ,  $K_B''$  and  $K_F''$  in order to obtain the colors  $K'''$ ,  $K_B'''$  and  $K_F'''$  (Fig. 14).

5 In a third step, the saturation of the chromatic shift is corrected according to the saturation difference between the reference color  $K$  and the color  $C_{ij}$ . For this purpose, the saturation difference ( $\Delta S_{CK}$ ) between  $C$  and  $K'''$  is computed using the relation

10  $\Delta S_{CK} = \text{sqrt}((F_{K'''} - E_C)^2 + (E_{K'''} - E_C)^2), \quad (5)$

and this saturation difference is added to  $K_B'''$  and  $K_F'''$  in order to obtain the colors  $C_b$  and  $C_f$  (Fig. 15).

15 In a fourth step, the CIE-Lab luminance difference between  $C_b$  and  $C_f$  is adjusted so that it is equal to the CIE-Lab luminance difference between  $K_b$  and  $K_f$  while maintaining the balanced average of  $C_b$  and  $C_f$  at color  $C_{ij}$

20 In a fifth step, the colors  $C_b$  and  $C_f$  are examined to see if they fit in the RGB color space. If this is not the case, the distance between  $C_b$  and  $C_f$  is proportionally reduced until both colors fit entirely into the RGB space (Fig. 16).

Applying the chromatic shift:

25 In a sixth step, the value  $p_{ij}$  of the security pattern pixel associated with the original image pixel is examined. If this pixel is white (e.g. corresponding to  $p_{ij} = 0$ ), and therefore belongs to the background of the security pattern, then the color  $C_b$  is assigned to the pixel of the original image. If this pixel is black ( $p_{ij} = 1$ ), and therefore belongs to the foreground of the security pattern, then the color  $C_f$  is assigned to the pixel of the original image. In general, for non-binary security patterns, the new color  $C_{ij}'$  is  
 30 calculated from

$$C_{ij}' = C_b(C_{ij}) \cdot (p_{ij} - p_{\min}) / (p_{\max} - p_{\min}) + C_f(C_{ij}) \cdot (p_{\max} - p_{ij}) / (p_{\max} - p_{\min}), \quad (6)$$

where  $p_{\min}$  and  $p_{\max}$  are the minimum and maximum possible pattern values  $p_{ij}$ .

#### Printing the modified image:

5       The modified image is output on a continuous-tone printer such as a dye-sublimation printer. Dithering devices that apply halftone screens on the images they print, such as laser printers or ink-jet printers, are not suitable for printing the protected images because  
10      the dithering process alters the structure of the embedded text.

#### Detection of the embedded text:

15      If the reference shift  $\{K, K_b, K_f\}$  presents a large enough contrast, the embedded text is readable under normal viewing conditions. Conversely, if the reference shift  $\{K, K_b, K_f\}$  presents a weak contrast, the embedded text is invisible and a close inspection or image analysis is required in order to read it.

20

#### Remarks:

25      The order of the various steps described above can be changed. In particular, the average values  $\alpha_k$  can be calculated after the security pattern of Fig. 9 is generated, and the steps for correcting the luminance, hue and saturation of the color shift are interchangeable.

30      The local averages  $\alpha_k$  have been calculated as the averages over the individual characters of the security pattern. It is, however, also possible to use other averaging techniques. In particular, the security pattern can be processed by a low pass filter, where each point is e.g. replaced by a weighted average of itself and a number of neighboring points.

35

As already indicated, the security pattern may be non-binary and can e.g. consist of various gray

levels, such as the may be used for representing anti-aliased characters.

In more general terms, the method described here starts from an original image and a security pattern. It calculates local averages  $\alpha_k$  of the values  $p_{ij}$  of the security pattern, e.g. by averaging over the bitmap of one character or by running the security pattern through a low pass filter or by using interpolation techniques of averaged values such as described by reference to Figs. 11 and 12. In particular, the local average  $\alpha_k$  of an area  $k$  can e.g. be calculated from

$$\alpha_k = \sum A_{k,ij} \cdot p_{ij} \quad (7)$$

wherein  $A_k$  is a matrix of weights and  $\sum$  is the sum over the points with indices  $i, j$  in said area  $k$ . In the example above, the area  $k$  corresponds to one character bitmap and  $A_{k,ij} = 1/N_k$ , wherein  $N_k$  is the number of points in said area.

For at least some of the points of the original image, the color  $C_{ij}$  of the original image is replaced by a color  $C'_{ij}$  using a function  $f$ :

$$C'_{ij} = f(C_{ij}, p_{ij}, \alpha_k),$$

wherein the function  $f$  depends on at least one local average  $\alpha_k$  of an area  $k$  said point  $p_{ij}$  is located in.

Preferably,  $f$  should have the property that if  $m$  and  $M$  are real numbers with  $m < \alpha_k < M$ , and wherein  $C_m = f(C_{ij}, m, \alpha_k)$  and  $C_M = f(C_{ij}, M, \alpha_k)$ , and if  $C_{ij}$  lies within a color space with a Euclidean metric and we define  $R_m$  as the Euclidean distance between  $C_m$  and  $C_{ij}$  and  $R_M$  as the Euclidean distance between  $C_M$  and  $C_{ij}$ , then for any value  $p_{ij}$  in the interval  $[m, M]$ , the Euclidean distance between  $C_{ij}$  and  $f(C_{ij}, p_{ij}, \alpha_k)$  lies within the interval  $[0, \max(R_m, R_M)]$ . In addition to this,  $f$  (if defined in analytic form) should be continuous.

In other words, for pattern values that are close to the local average,  $f$  should be such that the color of the original image is changed only slightly. In this way, the appearance of the protected image remains

globally identical to the appearance of the original image.

If an averaging technique according to Eq. (7) is used,  $f$  is preferably such that

$$\sum (A_{k,ij} \cdot f(C, p_{ij}, \alpha_k)) \approx C. \quad (8)$$

This again ensures that the average color of a given local area  $k$  of the modified image is equal to the average color of the same area of the original image.

Function  $f$  can be implemented algorithmically; e.g. by providing a chromatic shift for any given color  $C_{ij}$  and any local area  $k$ . The chromatic shift is given by two colors  $C_b(C_{ij})$  and  $C_f(C_{ij})$ , wherein the function  $f$  depends on said coverage-balanced chromatic shift in such a way that

$$\begin{aligned} f(C, p_{\min}, \alpha_k) &= C_b(C_{ij}) \text{ and} \\ f(C, p_{\max}, \alpha_k) &= C_f(C_{ij}), \end{aligned}$$

wherein  $p_{\min}$  and  $p_{\max}$  are the minimum and maximum possible pattern values  $p_{ij}$ . Between these values,  $f$  can e.g. be calculated by linear interpolation.

For calculating the chromatic shift for a given color  $C_{ij}$ , various methods can be used. As described above, it is e.g. possible to provide a reference shift for one reference color  $K$ . The reference shift is given by two colors  $K_b$  and  $K_f$ , wherein  $K$ ,  $K_b$  and  $K_f$  lie on a single line in an Euclidean additive color space and  $K$  is located in the center of  $K_b$  and  $K_f$ . The reference shift corresponds to the chromatic shift for color  $C_{ij}$  if  $C_{ij} = K$  and  $\alpha_k = (p_{\max} + p_{\min})/2$ . The reference shift can then be balanced e.g. using Eq. (2) above. Then, depending on the position of the colors  $K$  and  $C_{ij}$ , the values  $C_b(C_{ij})$  and  $C_f(C_{ij})$  can be derived by correcting hue, saturation and luminance, e.g. using Eqs. (3) - (5).

### Claims

1. A method for generating a security document by applying a security pattern to an original image  
 5 for generating a modified image, characterized in that  
     said security pattern comprises a plurality of points, wherein each of said points represents a pattern value  $p_{ij}$  and wherein local averages  $\alpha_k$  are calculated from said pattern values for at least some areas  $k$   
 10 of said security pattern, and

    wherein for at least some of the points in said security pattern the color  $C_{ij}$  of the corresponding point of the original image is replaced by a modified color  $C'_{ij}$  according to

15  $C'_{ij} = f(C_{ij}, p_{ij}, \alpha_k),$

wherein  $f$  is a function that depends on at least one local average  $\alpha_k$  of an area  $k$  said point is located in.

2. The method of claim 1, wherein said function  $f$  is such that

20 if  $m$  and  $M$  are real numbers with  $m < \alpha_k < M$ ,  
 and wherein  $C_m = f(C_{ij}, m, \alpha_k)$  and  $C_M = f(C_{ij}, M, \alpha_k)$ ,

    and if  $C_{ij}$  lies within a color space with a Euclidean metric and we define  $R_m$  as the Euclidean distance between  $C_m$  and  $C_{ij}$  and  $R_M$  as the Euclidean distance  
 25 between  $C_M$  and  $C_{ij}$ ,

    then for any value  $p_{ij}$  in the interval  $[m, M]$ , the Euclidean distance between  $C_{ij}$  and  $f(C_{ij}, p_{ij}, \alpha_k)$  lies within the interval  $[0, \max(R_m, R_M)]$ .

3. The method of one of the preceding claims,  
 30 wherein said function  $f(C_{ij}, p_{ij}, \alpha_k)$  is continuous in  $p_{ij}$ .

4. The method of one of the preceding claims, wherein said local averages  $\alpha_k$  are calculated as a weighted sum

35  $\alpha_k = \sum A_{k,ij} \cdot p_{ij}$

wherein  $A_k$  is a matrix of weights and  $\sum$  is the sum over the points with indices  $i, j$  in said area  $k$ , and

wherein said function  $f$  has the property that, for any color  $C$  of said original image in said area

$$\sum (A_{k,ij} \cdot f(C, p_{ij}, \alpha_k)) \approx C.$$

5        5. The method of claim 4, wherein all elements of said matrix  $A_k$  are equal to  $1/N_k$ , wherein  $N_k$  is the number of points in said area.

6. The method of claim 5, wherein said security pattern comprises a plurality of characters and wherein said local areas are rectangular areas, each of  
10        said rectangular areas enclosing one character.

7. The method of one of the preceding claims further comprising the step of providing a chromatic shift for any given color  $C_{ij}$  and any local area  $k$ , said chromatic shift being given by two colors  $C_b(C_{ij})$  and  
15         $C_f(C_{ij})$ , wherein said function  $f$  depends on said coverage-balanced chromatic shift such that

$$f(C, p_{\min}, \alpha_k) = C_b(C_{ij}) \text{ and}$$

$$f(C, p_{\max}, \alpha_k) = C_f(C_{ij}) \text{ and}$$

for  $p_{\min}$  and  $p_{\max}$  being the minimum and maximum possible  
20        pattern values  $p_{ij}$ .

8. The method of claim 7, wherein

$$f(C_{ij}, p_{ij}, \alpha_k) = C_b(C_{ij}) \cdot (p_{ij} - p_{\min}) / (p_{\max} - p_{\min}) \\ + C_f(C_{ij}) \cdot (p_{\max} - p_{ij}) / (p_{\max} - p_{\min})$$

9. The method of claim 8 further comprising  
25        the steps of

choosing a reference shift for a reference color  $K$ , wherein said reference shift is given by two colors  $K_b$  and  $K_f$  and corresponds to said chromatic shift for said color  $C_{ij}$  if  $C_{ij} = K$  and  $\alpha_k = (p_{\max} + p_{\min})/2$ ,

30        calculating said chromatic shift for any other color  $C_{ij}$  from said reference shift by transforming said two colors  $K_b$  and  $K_f$  as a function of color  $C_{ij}$  and said local averages  $\alpha_k$ .

10. The method of claim 9, wherein said reference color  $K$  and said two colors  $K_b$  and  $K_f$  are arranged  
35        on a line in an Euclidean, additive color space, wherein

$K_b - K = K - K_f$  and wherein said step of calculating said chromatic shift comprises the steps of

calculating first corrected colors  $K_b'$  and

$K_f'$  from

$$K_b' = K_b + d$$

$$K_f' = K_f + d$$

with

$$d = (K_f - K_b) \cdot (\alpha_k - (p_{\max} - p_{\min})/2) / (p_{\max} - p_{\min}),$$

and calculating said two colors  $C_b(C_{ij})$  and

$C_f(C_{ij})$  from said first corrected colors  $K_b'$  and  $K_f'$ ,  
said reference color  $K$  and said color  $C_{ij}$ .

11. The method of one of the claims 9 or 10 comprising the step of calculating said two colors  $C_b(C_{ij})$  and  $C_f(C_{ij})$

by correcting the luminance of the chromatic shift according to the luminance difference between the reference color  $K$  and the color  $C_{ij}$ , and/or

by correcting the hue of the chromatic shift according to the hue difference between the reference

color  $K$  and the color  $C_{ij}$ , and/or

by correcting the saturation of the chromatic shift according to the saturation difference between the reference color  $K$  and the color  $C_{ij}$ .

12. The method of claim 10 or 11 comprising the step of correcting a CIE-Lab luminance difference between said two colors  $C_b(C_{ij})$  and  $C_f(C_{ij})$  to make it equal to the CIE-Lab luminance difference between said two colors  $K_b$  and  $K_f$ .

13. The method of one of the preceding claims wherein said pattern values are binary having values of 0 and 1, wherein for a pattern value of 0 the color  $C_{ij}$  of the corresponding point of the original image is shifted in a first direction and for a pattern value of 1 the color  $C_{ij}$  of the corresponding point of the original image is shifted in a second direction, and in particular wherein, in a given Euclidean color space, said first direction is opposite to said second direction.



14. The method of one of the preceding claims wherein said original image is a holder's photograph on an identity document.

5 15. The method of one of the preceding claims comprising the step of printing the modified image on a continuous-tone printer.

16. A security document obtainable by the method of one of the preceding claims.

10 17. The security document of claim 16, wherein said security document is a driving license.

15 18. The security document of one of the claims 16 or 17, wherein said pattern is a text representing information that is also elsewhere visible on said document, and in particular wherein said text is at least partially encrypted.

### Abstract

The described method is used for generating a security document by applying a security pattern to an original image. The security pattern comprises a plurality of points, wherein each of said points represents a pattern value. Local averages are calculated from said pattern values for at least some areas of the security pattern. For at least some of the points of the security pattern the color of the corresponding point of the original image is replaced by a modified color. The modified color is a function of the local average, the original color and the corresponding pattern value. The method provides good security against counterfeit because it is difficult to implement using conventional image processing applications. For a suitable choice of the color transformation function, the resulting image can preserve the local color tones of the original image.

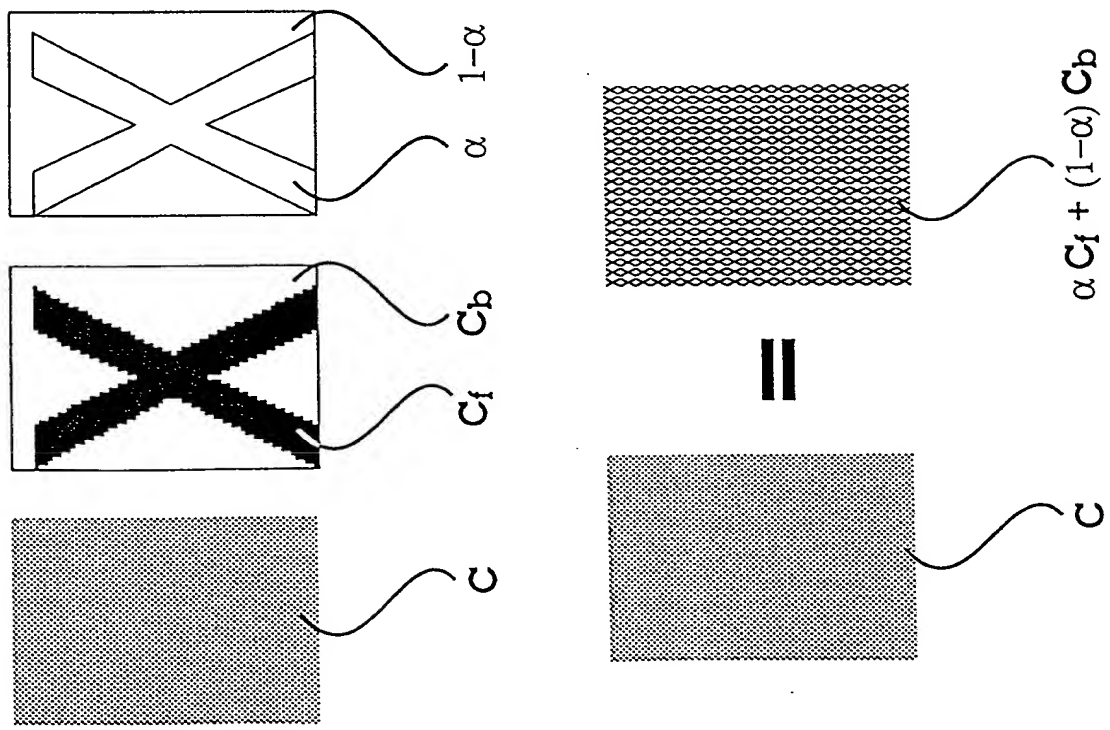


Fig. 1

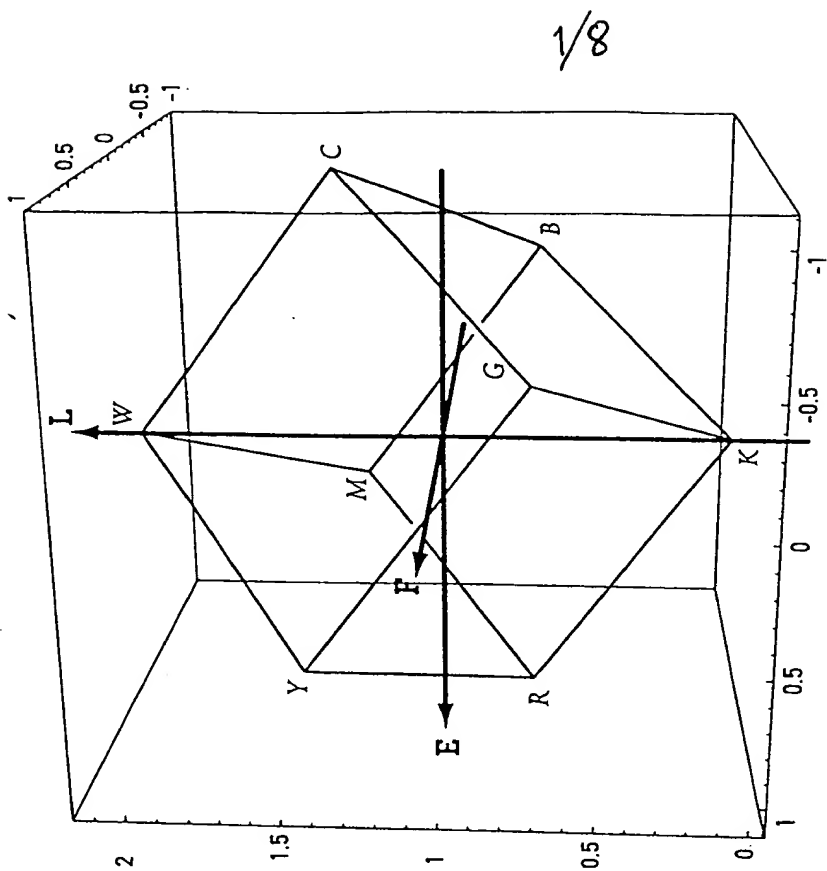


Fig. 2

2/8

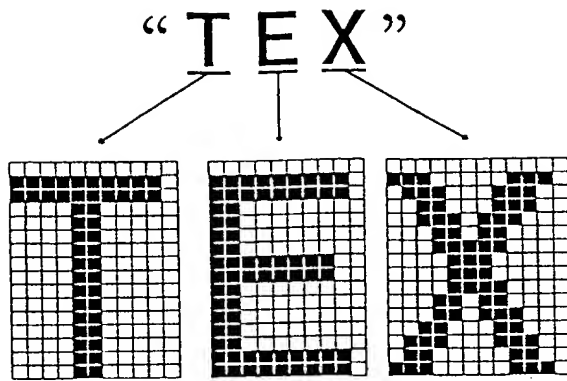


Fig. 3

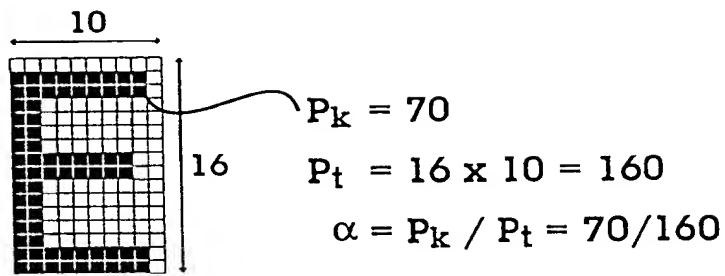


Fig. 4

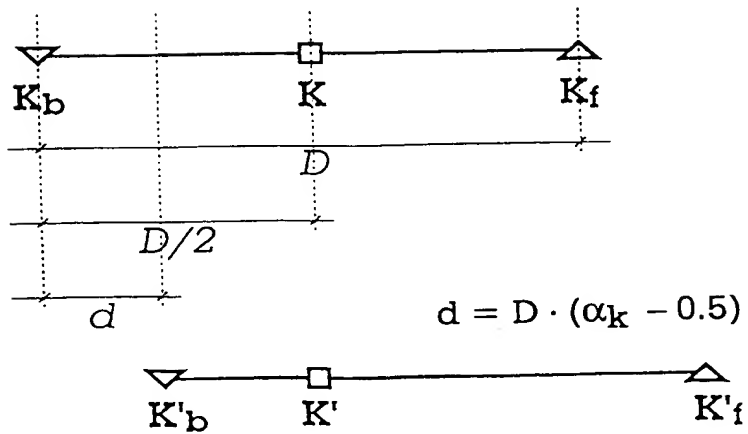


Fig. 5

3/8

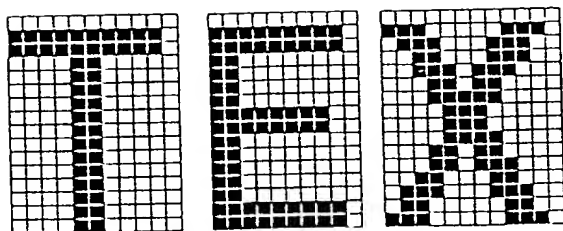


Fig. 6

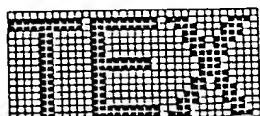
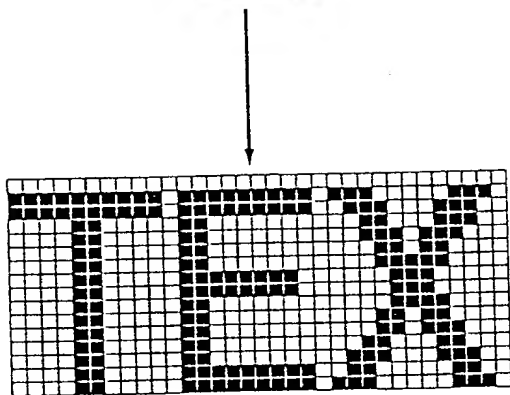
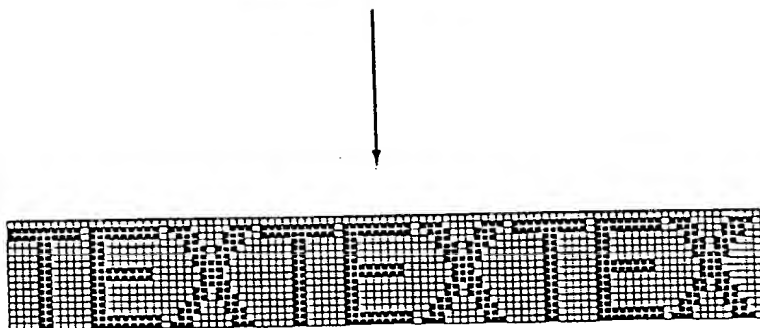
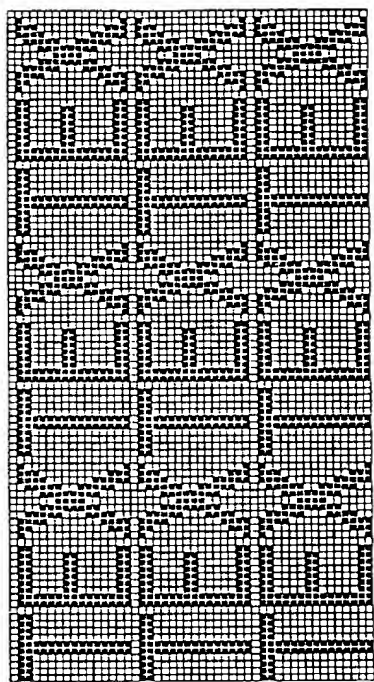


Fig. 7





4/8

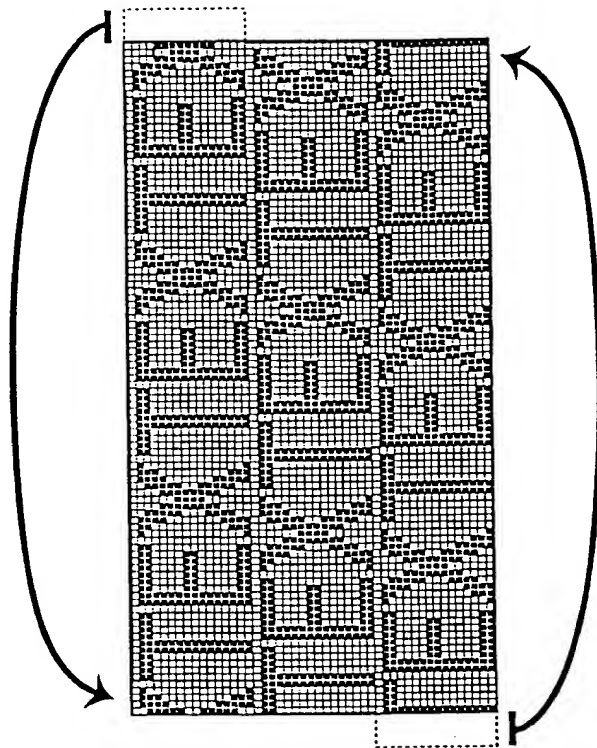


Fig. 9

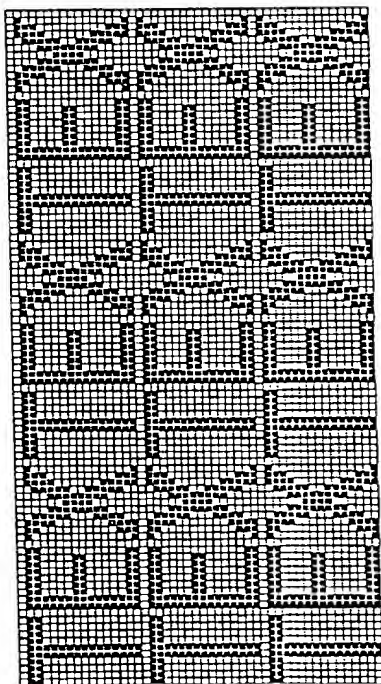
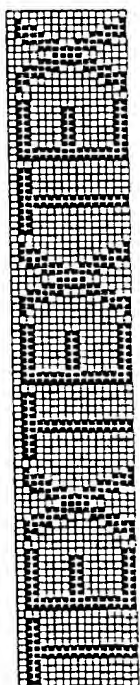


Fig. 8

5/8

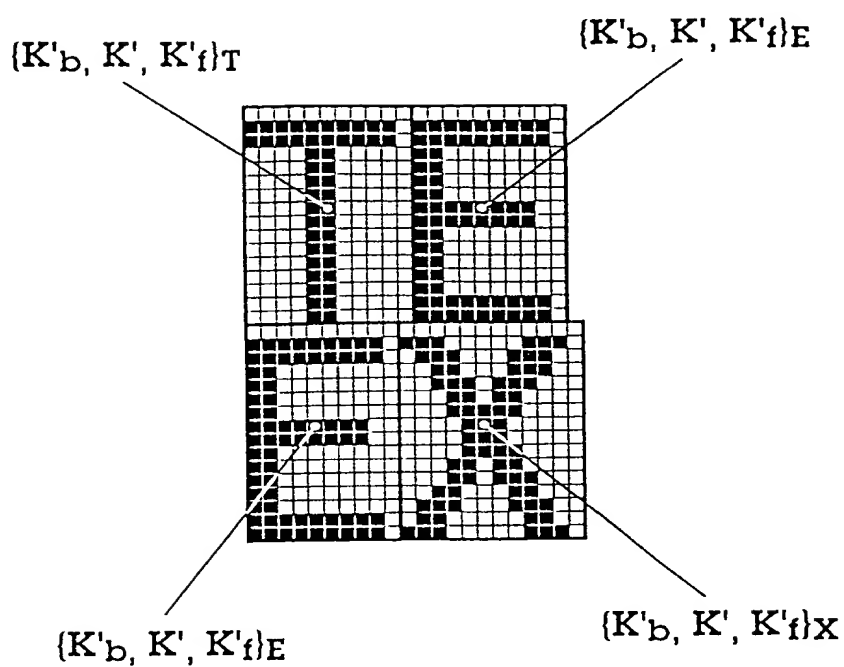


Fig. 10

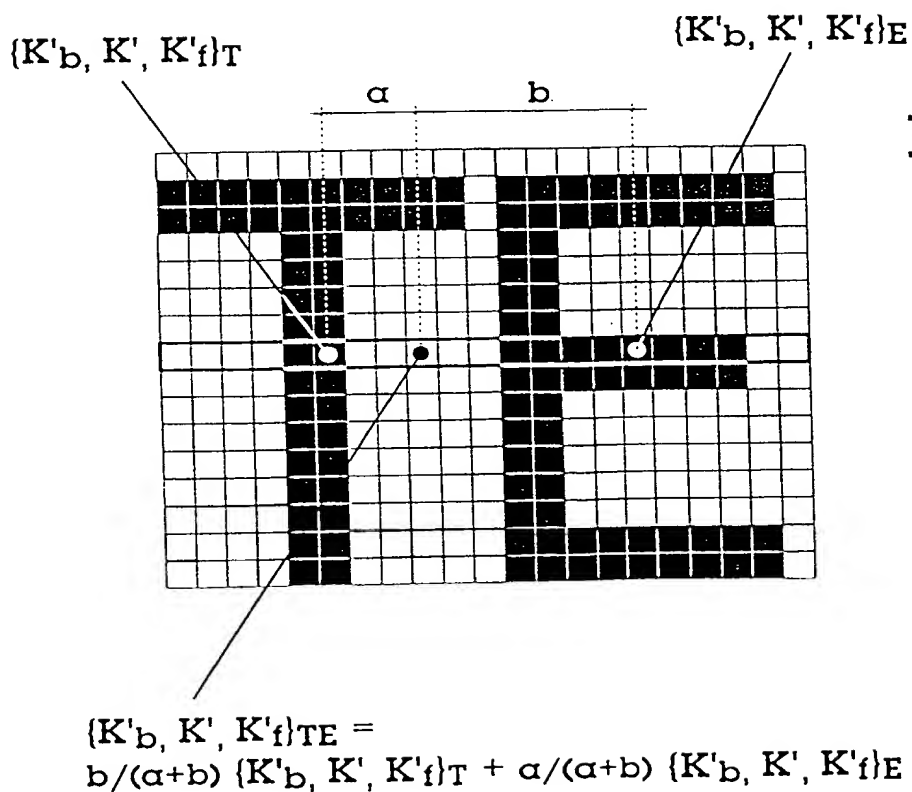


Fig. 11

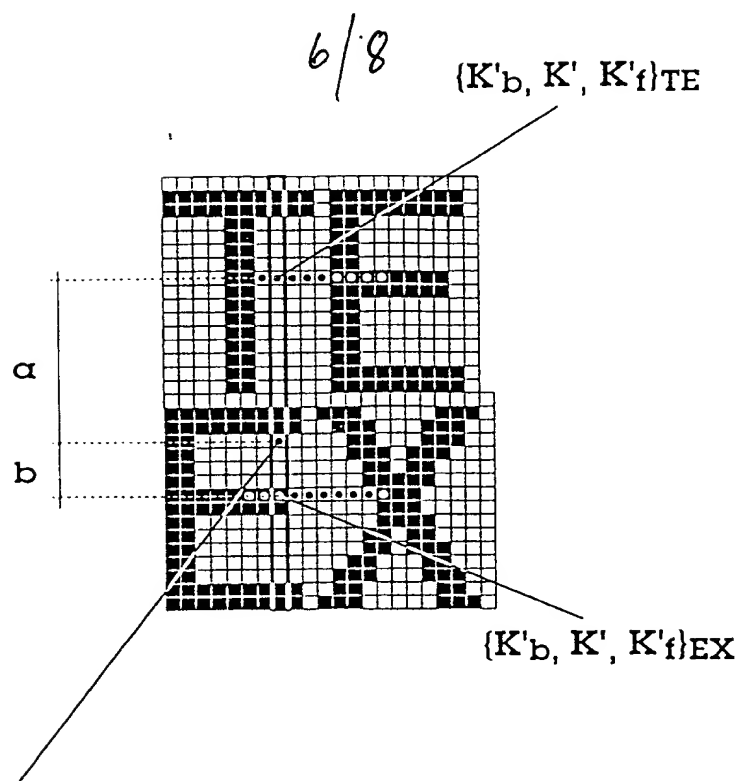


Fig. 12

$$\{K'_b, K', K'_f\} = \frac{b}{(\alpha+b)} \{K'_b, K', K'_f\}_{TE} + \frac{\alpha}{(\alpha+b)} \{K'_b, K', K'_f\}_{EX}$$

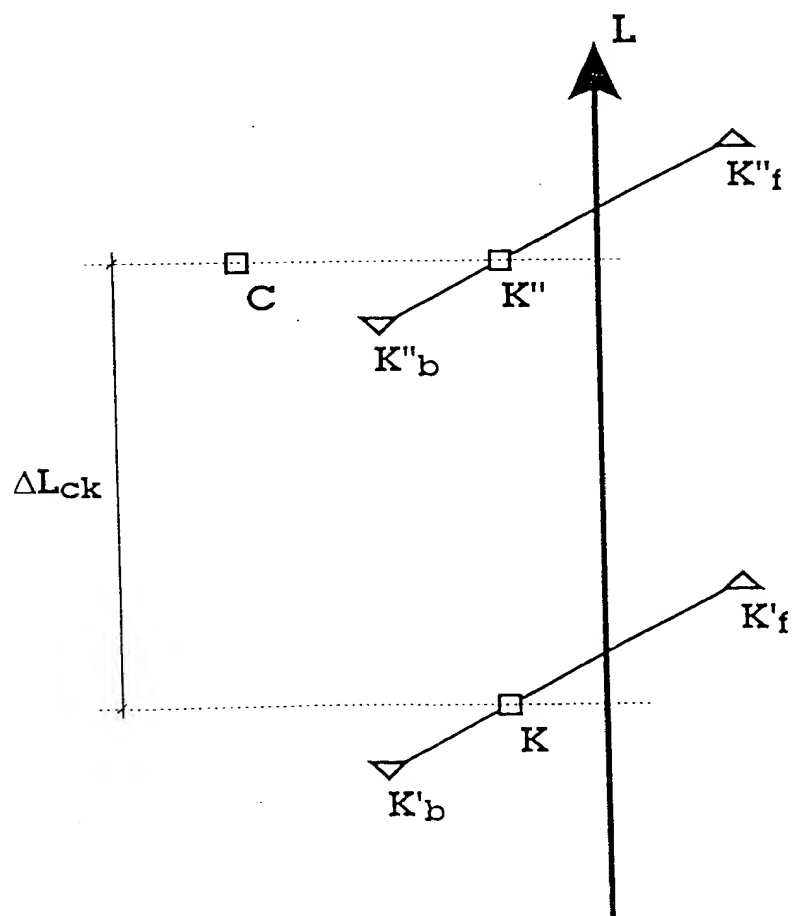


Fig. 13



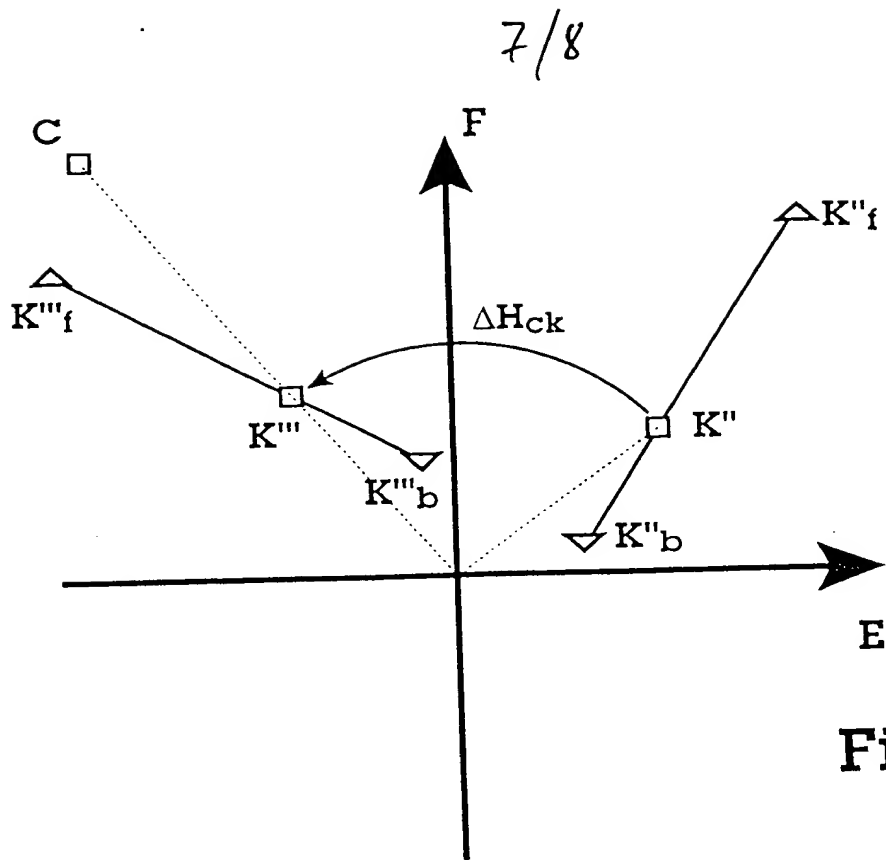


Fig. 14

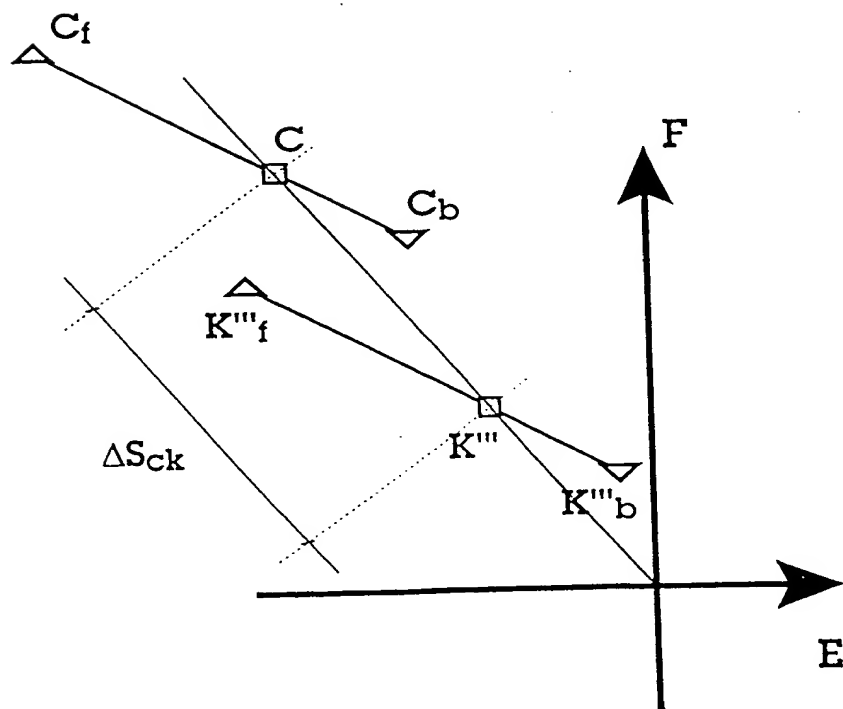


Fig. 15

8/8

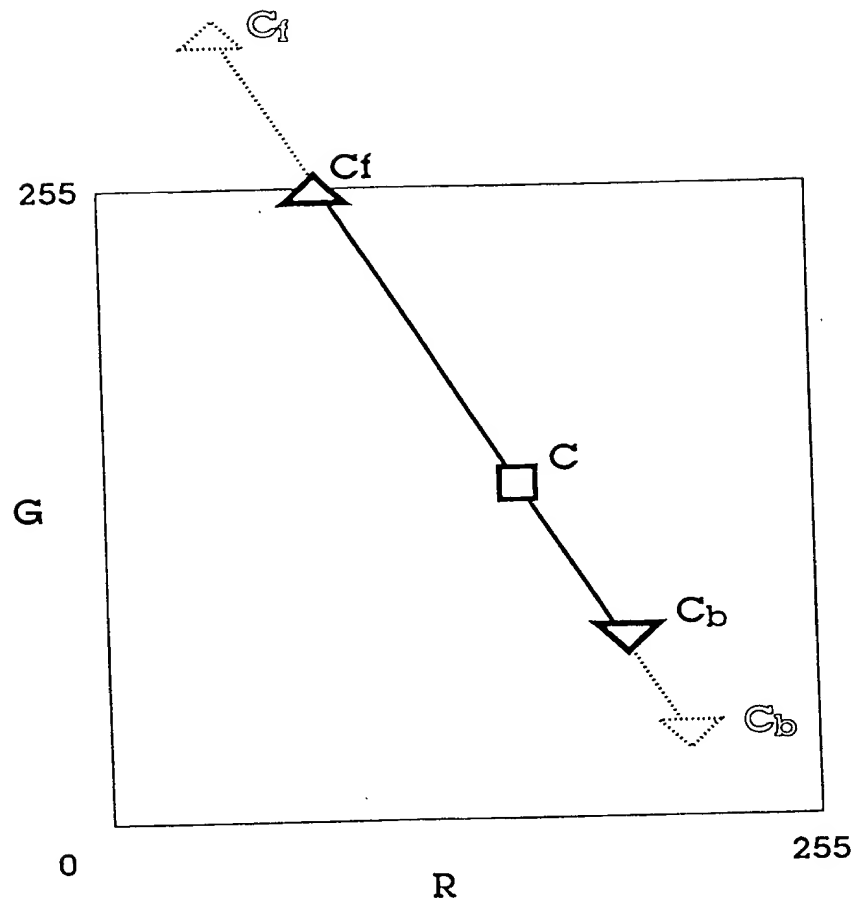


Fig. 16